INTERNAL AUDIT REPORT

Review of Remote Access Dial-up Security

Fairfax County Internal Audit Office

FAIRFAX COUNTY, VIRGINIA
INTERNAL AUDIT OFFICE
MEMORANDUM

TO: Anthony H. Griffin
County Executive

DATE: October 13, 2000

FROM: Ronald A. Coen, Director
Internal Audit Office

SUBJECT: Report on the ***"Review of Remote Access Dial-Up Security Audit"***

This is a report on the ***"Review of Remote Access Dial- Up Security Audit".*** It was performed as part of our FY2000 Annual Audit Plan.

The findings and recommendations of this audit were discussed with the Department of Information Technology. We have reached agreement on all of the recommendations and I will follow up periodically until implementation is complete. Their responses are incorporated into the report and the full response is attached at the end of the report. After your review and approval, we will release the report to the Board of Supervisors.

RAC:dh

TABLE OF CONTENTS

Introduction

In Fiscal Year 1995, the County created a Telecommuting Pilot program and installed the first communication security device to monitor remote access dial-up security. Telecommuters are employees that were authorized to work from their home, however not all telecommuters are remote access users. Currently, 15 percent of all remote users are telecommuters. The other 85 percent are made up of vendors, employees that work at remote sites using remote access as an alternative means to access the County's Enterprise system, and employees that are on travel.

During the County's Year 2000 effort, all County systems were evaluated for Year 2000 compliance. At this point it was discovered that the CompuSafe system (County's former dial-up access system) was not Year 2000 compliance, which led to efforts to find a replacement security system that meets the County's needs in addition to being Year 2000 compliance.

In 1999, the County selected the security system called Remote Access Control Module (ACM) from RSA Security, formerly Security Dynamics Technologies, Inc. Implementation of the new remote access system took place at the end of Calendar Year 1999. It became operational in January 2000. This system is a token-based user authentication system, using the RSA SecurID Authenticators (token cards). The ACM feature include authentication, access logging, RSA SecurID card database management, and report generation. ACM is used in conjunction with the RSA Access Control & Encryption (ACE) Server, which is designed for client/server environment security, focusing on authentication of user identity and manages user access.

The Information Protection Branch of DIT is responsible for the administration of the ACE Server application. Two Information Security Analysts were assigned to support the ACE Server, one is designated as the ACE Server Administrator and the other acts as the backup administrator. The Branch Manager as well as other staff are trained and have the expertise to support the ACE Server functions. The ACE Server Administrator and the County's Technical Support Center supports about 700 dial-up remote access users.

Purpose and Scope

This audit was performed as part of our FY 2000 long-range audit plan. The main objective of this audit was to perform a post implementation review of the security authentication system for dial-up access. This would include determining that the County's Information Protection Manual and the Remote Access Security Policy is current and applicable; and user departments are in compliance with County policy and procedures for remote access.

The scope of our audit is to:

- Review the use of the product's overall capabilities
- Understand the process of user identification and authentication
- Review procedures on security administration and monitoring of user activities
- Assess as to the completeness of the Information Protection Manual and Remote Access Security Policy as it relates to the current process
- Assess the cost vs. volume of remote access transactions

Methodology

We worked with the Information Protection Branch to understand the County’s process and procedures for dial-up access. We also interviewed the ACE Server Administrator to obtain an understanding of the features available with the ACM’s ACE Sever. We randomly selected 10 percent of all dial-up users and tested for completeness in authorization and procedure. We verified that the tested users are current users and are actively dialing into the network.

This audit covered the period of April 2000 through June 2000 and was conducted in accordance with generally accepted government auditing standard and the Government Accounting Office Federal Information System Controls Manual (January 1999).

Executive Summary

The implementation of the ACE Server, used for dial-up access, was successful. Currently over 700 users are remotely dialing into the County's network. Internal controls surrounding the remote access process are adequate. However, there are areas where enhancements are required.

- There is a sharing of the ACE Server administrative user ID and password by the Information Security Analysts and the Branch Manager. It is important that there be accountability to the changes or transactions made to the ACE Server. Sharing the administrator user ID would make it difficult to provide complete accountability.

- There is lack of separation of duties (incapable functions) between administrating user profiles and reviewing administrative changes to the application. The ACE Server Administrator reviews the system activity log daily. However, the Administrator also performs changes to the system. The Branch Manager reviews the activity log but not on a regular basis.

- The Remote Access Security Policy has been in draft form for over a year. To keep up with the increases in telecommuters, the County needs to provide a clear understanding of County policy on dial-up access security to all departments and/or users.

- The current version of the ACE Server does not allow for customized reports to be generated. However, an upgrade to this system will allow for report writing features. This would provide for more efficient monitoring of user activities and various transactions that affect the County's network.

Comments and Recommendations

1. The two ACE Server Administrators and the Branch Manager share the same administrator user ID and password for the RSA ACE Server.

The ACE Server Administrator, the backup Administrator, and the Branch Manager share the same administrator user ID and password to access the ACE Server system. This allows for minimal accountability to changes made to the system. Administrators should have their own user ID and password with specific assigned administrator role. By having individual user ID, it will allow for tracking of various transactions made to the system.

The ACE Server Administrator performs all daily monitoring and support to all dial-up access users. The Branch Manager and the backup person to the ACE Server Administrator provide additional monitoring or reviewing. Therefore, transactions created by each person should be closely monitor or reviewed.

As referenced in the ACE Server Administration Student Guide (Section7), users can be assigned administrator roles using their own user ID and password. This feature is included in the upgraded version of the application. Each administrator can also have specific task list that allows him or her to perform certain functions within their scope. Customizing the administrator's task lists and assigning individual user ID allows for separation of duties and accountability of changes made to the ACE Server.

Recommendation

The Information Protection Branch should explore the features available in the upgrade version of the ACE Server for separate administrative user ID. Each administrator and the Branch Manager should be assigned individual user ID and passwords to the ACE Server. This will allow for accountability of changes to the system and efficient monitoring of administrative transactions.

Department Response

The Information Protection Branch will install the most current version of ACE Server Administration software package by October 20, 2000. Subsequently, a more granular log-on process for the ACE Server Administrators will be established by October 31, 2000.

2. There is lack of separation of duties between administrating user profiles and reviewing the changes made to the ACE Server.

The ACE Server Administrator assigns token cards to users, creates a unique PIN for each user and issues the PIN to the user. The ACE Server Administrator also enables the user for dial-up ability and monitor of user transactions. In addition, the ACE Server Administrator maintains a database on all users and token cards, reviews the daily activity report, and follows-up on suspected or known violations. Overall, the ACE Server Administrator has the capacity to create, reset, or delete user profiles and change application settings. All administration activities are logged on the activity log. However, the log is not reviewed on a regular basis by someone other then the ACE Server Administrator.

Due to limited resources, there is one person assigned as the main ACE Server Administrator for ACE Server. In addition, there is another person that acts as backup to the ACE Server Administrator. There should be an independent person reviewing the activity log on a regular basis to ensure that there are no unusual transactions. The review should concentrate on changes made to the remote access application.

Recommendation

The Branch Manager should review the activity logs regularly for unusual transactions and violations to enhance preventative controls. This should be done at least on a weekly basis. This would allow changes made by the administrator to be reviewed. Preventative controls deter or minimize the occurrence of computer-related fraud, possible errors, omissions, and irregularities.

Department Response

The Information Protection Branch Manager will perform weekly reviews of the logs. This will be effective on October 13, 2000

3. The County does not have an approved Remote Access Security Policy. It has been in draft form for over a year.

The County currently does not have an approved Remote Access Security Policy for users. This policy has been in draft form for over a year mainly because of the installation of the ACE Server in 1999. In addition, the system will be upgraded shortly. However, the County should have a Remote Access Policy available for all remote access users. The policy manual should act as a reference for both user and the ACE Server Administrator. With as many as 700 remote access users, lack of a policy manual may create weaknesses in the controls around the remote access process.

Recommendation

The Remote Access Security Policy needs to be completed and presented to users by the end of calendar year 2000. The policy should provide a clear understanding of users and administrator as to the policy and procedures for using remote access through out the County.

Department Response

The Information Protection Branch will prepare a draft policy document on the authentication of Dial-up Remote Access by November 30, 2000. The draft policy should be finalized into a comprehensive formal policy by December 31, 2000. In addition, the finalized policy would be submitted to DIT Director for review and approval by January 15, 2001.

4. Customized reports should be generated to provide more efficient monitoring of user profiles and daily activities on the ACE Server.

The ACE Server records all information on the Activity Log. The standard reports available are the Activity, Exception, Incident, and Usage Summary reports. However, these reports can not be easily extracted to hard copies. In addition, customized reports can not be easily created to provide for efficient monitoring of activity.

From the information captured in the Activity Log, the application should be allow for customization of reports for specific monitoring purposes. Having these reports available on-line and/or as hard copies could be most beneficial. Examples of reports that may be useful in monitoring remote access would be a report on users with redundant violations in a week, users that have not signed-on in over 60 days, or multiple violations in/around a certain time frame.

The ACE Server's Activity Log captures all necessary information for monitoring users and activities. However, because this version of the application lacks the report writing feature, this limits the use of recorded information to assist in monitoring and/or preventing unauthorized access to the ACE Server.

At the time of the initial purchase, the County obtained the most current version of the ACE Server application. However, this version did not have the ability for customized reporting. The upgraded version that came out does include the reporting feature.

Recommendation

The Branch Manager and the ACE Server Administrator attended training to provide them with information on the upgrade to the ACE Server application. Information Protection Branch will install the upgrade as soon as possible. Once the upgrade is installed, customized reports can be generated to assist in the monitoring process. This will help in providing a management trail of transactions that took place on the server and improve the monitoring process of remote users.

Department Response

Once the upgraded ACE Server version is installed, the Information Protection Branch will explore reporting capabilities. The milestone date for the exploration of reporting capabilities is December 31, 2000. In addition, required reports will be generated by January 15, 2001.